REMARKS

Summary of the Office Action

Claims 1-8, 12-15, 19-25, 27-39 are currently pending and at issue in the present application. Applicant respectfully submits no new matter has been added by this Reply. Claims 1-39 are rejected.

Claims 1-8, 12-15, 19-25, 27-39 are rejected under 35 U.S.C. §101; Claims 1-39 are rejected under 35 U.S.C. §102(b) as unpatentable over U.S. Patent 6,396,926 to Takagi et al. (hereinafter referred to as "Takagi"). Applicant request reconsideration of these rejections, in light of the amendments and the below remarks.

Rejection Under 35 U.S.C. §101

Examiner has rejected Claims 1-8, 12-15, 19-25, 27-39 under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter.

35 U.S.C. 101 states:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefore, subject to the conditions and requirements of this title.

Substantive Rejection Under 35 U.S.C. §102

Examiner has rejected Claims 1-8, 12-15, 19-25, 27-39 under 102(b) as anticipated by Takagi

35 U.S.C. 102(b) states:

> A person shall be entitled to a patent unless–
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Cited Art – Takagi Patent

The Examiner indicates that the Takagi reference teaches a method for decrypting a ciphertext obtained from a plaintext using a first and second public key, by applying the Chinese remainder theorem (claim 1). The public key N, or public modulus N, is generated from private keys by **at least squaring** one of the private keys, thus making the public modulus N a **squareful number**. Further, Takagi describes an authentication method for verifying the sender-receiver message (claim 5); a decryption apparatus (claim 9); a cipher communication system, comprised of a sender apparatus for the encryption/decryption key generation processing unit, and a receiver apparatus containing a calculation processing unit, and a decryption processing unit (claim 10); an authentication message sender apparatus, comprising an encryption/decryption key generation processing unit, an authentication message hashing processing unit, and an authentication encryption processing unit (claim 11).

Limitations of Rejected Claims

The independent claims were amended to clarify the present invention and to overcome the rejections of the examiner, for substantive rejections.

Applicant's Cryptographic Communication Device

Applicant's invention provides systems and methods for encryption of messages using a public and private key cryptosystem. In a method for secure communication or transmission of electronic matter, according to the present invention, wherein the matter is encrypted and decrypted using RSA methods including the steps of: providing at least two private keys and at least one public key for decrypting an electronic communication or transmission, wherein the at private keys are based upon a multiplicity of **distinct** primes that, when multiplied produce a corresponding one of the at least one public key that is **not a squareful number**;

encrypting/decrypting the communication or transmission using the at least one public key; and providing at least two private keys capable of decrypting/encrypting the communication or transmission using a single one of any of the at least two private keys. There is structure provided in the amended claims, including a computer and/or computer-type device capable of communicating on a network (supported by originally filed specification, including page 19) to address the claims rejections under 101 and 112.

Analysis of Cited Art to Rejected Claims

Takagi describes a method of encryption that generates a **squareful** modulus as the product of a series of **distinct** prime factors wherein one of the prime factors is raised to an exponent k, thus generating a product from **non-distinct** prime factors. Takagi then teaches the decryption of the encoded message using **all** of the **distinct** prime factors. The present invention, instead, teaches the generation of a **squarefree** modulus and the decryption of the resulting encoded message using **less than all** of the **distinct** prime factors. The claims have been amended to distinguish over the prior art.

Response to Arguments

The Examiner has indicated that the applicant's arguments and amendments are not persuasive, but does not offer any reasoning to specifically rebut the amendments and arguments for a **squarefree** modulus and using less than all of the **distinct** prime factors to decode a message.

Examiner merely restates that a method that uses less than all of the prime factors for the modulus is known:

"As a result, the system of cited prior art does implement and teaches a public key cryptography schemes to allow for decryption of messages using less than all of the prime factors of the modulus that is used for encryption of the messages."

Applicant respectfully reasserts that the combination of using less than all of the **distinct** prime factors of a **squarefree** modulus is a novel and bona fide limitation. It is a bona fide limitation because limiting the modulus to a squarefree modulus makes Takagi's method inoperable. Thus, the applicant's invention is a further limitation on the method of using less than all of the prime factors of the modulus.

The reason Takagi's method is inoperable with the Applicant's method is that Takagi's method, while on the surface appearing to use less than all the prime factors, in reality does not. In reality, Takagi's method uses the same factor twice to create the first secret key. Takagi uses $n=p^kq$ to generate a first private key. For example, If k=2, then the prime factors are p * p * q to generate the modulus N. Takagi then uses p only once (along with q) to decipher an encrypted message. Arguing that Takagi's method allows for decryption of messages using less than all of the prime factors is a question of semantics. That is, if we use p multiple times to encrypt, but then use it fewer times to decrypt, we have really not used p any less, because we will have to use the fewer p's more times to achieve the same decryption result as using all the p's. Thus, Takagi does not really teach using less than all the prime factors.

Additionally, the Applicant has overcome this argument by limiting the use of the prime factors in decryption to the use of less than all of the **distinct** prime factors.

As one of ordinary skill in the art would recognize, and consistent with the examiner's reaching beyond specification, the definition of squareful includes squares, the definition of

squarefree does not. The Examiner does not address this limitation, either. Takagi uses a squareful modulus, but cannot use a squarefree modulus.

The present invention provides for **improving the computational efficiency** of RSA systems, specifically through the **faster decryption** of RSA-encrypted messages, as stated in the specification:

[0032] The present invention discloses methods for **improving the computational efficiency and overall capabilities** of RSA and related public key cryptographic systems. In prior art, decryption of messages that are encrypted using a public key {e, N} is always achieved using all of the distinct prime factors of N. For example, the private exponent d is usually calculated such that e*d=1 mod Z, where Z is the product of each of the prime factors of N minus 1. In addition, RSA implementations that employ the Chinese Remainder Theorem (CRT) also use each of the distinct prime factors of N as moduli in small modular exponentiations that are combined to perform decryption. The present invention discloses several methods where the prime factors used for decryption are a proper subset of the prime factors in the modulus N, or the prime factors of the modulus used for encryption are a proper superset of the prime factors used for decryption. The techniques proposed in the present invention not only **provide for a substantial increase in the computational speed of RSA decryption,** but **also open the door for exciting new applications of public key cryptography**.

The present invention also provides for **faster decryption with respect to the method of Takagi** because of the reduction in the number of absolute and distinct prime factors used in decryption with respect to the method of Takagi. Takagi still requires a minimum of at least two prime factors for decryption. Take for example three prime numbers p, q, and r where p, q, and r

are all distinct prime numbers. The present invention allows decryption using just one of the three distinct prime numbers p. In Takagi's method, the public key would be the product of p, p, and r (only two distinct prime factors). Decryption would be performed not only on p but also r.

Applicant respectfully request reconsideration. This is clearly an oversight by the examiner maintaining the rejection without addressing the two limitations.

In order for a reference to act as a §102 bar to patentability, the reference must teach each and every element of the claimed invention. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 771 (Fed. Cir. 1983).

The present invention systems and methods for encrypting/decrypting messages operable on a computer system, computer-type device and/or computer network provide the activity on a machine and/or product, including the steps of: providing a public key cryptosystem including a computer operable to generate at least one key for encrypting/decrypting at least one message, the public key cryptosystem having a predetermined number of **distinct** prime factors used for the generation of a **squarefree** modulus N and an exponent e; wherein a proper subset of **less than all** of the **distinct** prime factors of the modulus N are used to decrypt messages that are encrypted using the public exponent e and the public modulus N, where e and N are calculated using RSA methods, and encryption of the message occurs using RSA methods. These steps and others in the independent claims, now amended, are not included in the Takagi patent.

Without the required teaching of each element as set forth in the claims, it is improper for the Examiner to continue such rejections under §102(e). Therefore, Applicants respectfully request withdrawal of this rejection as to independent Claims 1, 2, 3, 5, 12, 13, 19, 23, 27, 30, 31, 34, 35, 36, 37, 38 and 39. Further, because remaining claims depend from one of these

independent claims, adding additional limitations to each, the rejection of these dependent claims under § 102(e) should also be withdrawn. Applicant respectfully requests that the rejections be withdrawn as to Claims 1-39 and those claims allowed.

CONCLUSION

The Office Action of October 7, 2010, has substantively rejected Claims 1-8, 12-15, 19-25, 27-39 are rejected under 35 U.S.C. §101; Claims 1-39 are rejected under 35 U.S.C. §102(b) as unpatentable over Takagi. The amendments and remarks of Applicant address these rejections. Accordingly, Applicant believes the claims are in condition for allowance. Reconsideration of the pending objections and rejections is respectfully requested, and a notice of allowance is respectfully sought. If any issues remain outstanding, incident to the allowance of the application, Examiner Zia is respectfully requested to contact the undersigned attorney at (919) 268-4236 or via email at jinan@trianglepatents.com to discuss the resolution of such issues, in order that prosecution of the application may be concluded favorably to the applicant, consistent with the applicant's making of a substantial advance in the art and particularly pointing out and distinctly claiming the subject matter that the applicant regards as the invention.

Respectfully submitted,

JiNan Glasgow, Reg. No. 42585

Triangle Patents
PO Box 28539
Raleigh, NC 27611-8539
919-268-4236 phone